JURNAL DIGITAL TEKNOLOGI INFORMASI
Vol. 06, No. 02, September 2023, pp. 76-81
E-ISSN 2714-9706 | P-ISSN 2686-4185
Terakreditas Sinta 5 oleh Dirjen Pendidikan Tinggi, Riset, dan Teknologi No. 164/E/KPT/2021

Analisis kejahatan phising pada sektor e-commerce di marketplace shopee

Devi Puspitasari [a,1,*]; Tata Sutabri [a,2]
[a] Universitas Bina Darma, Jl. Jenderal Ahmad Yani No.3, 9/10 Ulu, Kecamatan Seberang Ulu I, Palembang dan Indonesia
[1] puspitas.devi0498@gmail.com; [2] tata.sutabri@gmail.com
** Corresponding author*

Artikel Histori: Diterima 26/01/2023; Revisi 09/09/2023; Terbit 09/09/2023

Abstrak

Cybercrime merupakan kejahatan yang dilakukan dengan menggunakan teknologi komputer sebagai kejahatan utama. Kejahatan yang terjadi di zaman modern ini semakin berkembang dan berbagai kejahatan yang terjadi saat ini juga telah masuk ke dunia maya dalam bentuk kejahatan phising. Kejahatan phising adalah ancaman yang menggunakan teknik manipulatif dan menipu pengguna dengan menyamar sebagai orang yang berwenang, vendor atau peserta e-commerce untuk mendapatkan informasi sensitif pengguna. Penelitian ini membahas tentang faktor penyebab phising dan mencegah ancaman serangan phising yang terjadi pada sektor e-commerce. Metode yang digunakan adalah metode literature review. Faktor penyebab phising adalah minimnya pengetahuan pengguna, penambangan data pengguna, menarik pengguna dengan hadiah, dan sebagainya. Meskipun pencegahan dapat dicapai dengan mengedukasi pengguna, hal ini dapat menghindari ancaman kejahatan phising di email,URL atau situs web dan lain-lain.

Kata Kunci: Cybercrime, Phising, E-Commerce.

Pendahuluan

Di era teknologi informasi dan komunikasi sekarang ini, segala sesuatu dapat dilakukan dengan mudah dan cepat. Hampir semua bidang kehidup¬an tidak lepas dari teknologi informasi dan komunikasi. Hal ini disebabkan adanya teknologi internet yang memudahkan pertukaran informasi yang cepat antar manusia dan komunikasi jarak jauh. Dengan adanya teknologi internet saat ini dapat memudahkan pengguna untuk mengakses website atau aplikasi online sehingga memungkinkan pengguna dalam melakukan aktivitas salah satunya adalah melakukan transaksi jual beli (e-commerce) secara online.

Penggunaan situs e-commerce untuk belanja online saat ini sudah menjadi kebutuhan utama masyarakat Indonesia, hal ini didukung oleh Pratama Afrianto & Irwansyah (2021) bahwa belanja online sudah menjadi gaya hidup masyarakat Indonesia. Menurut Hadya Jayan (2021), penjualan e-commerce akan mencapai $53 miliar pada tahun 2021, karena teknologi informasi dapat memberikan peluang bagi penjual untuk menjangkau pembeli dalam skala yang lebih besar.

Layanan belanja online membawa keuntungan bagi penjual dan pembeli, sebaliknya penggunaan layanan tersebut menimbulkan dampak negatif. Salah satu penyalahgunaan layanan e-commerce dalam teknologi internet adalah phising. Ginanjar dkk. (2018), kejahatan phising dapat dilakukan dengan menggunakan teknik desain situs web, yang mengakibatkan kerugian finansial, pencurian identitas, dan pelanggaran akun.

Phising adalah istilah yang mengacu pada berbagai kejahatan dunia maya dengan memberikan tautan kepada pengguna internet yang berupaya mencuri informasi pribadi seperti detail bank, kode PIN, dan informasi media sosial. Cara umum untuk mengelabui pengguna online adalah dengan menawarkan tautan atau pesan email. Aktivitas phising telah menarik penelitian di komunitas keamanan Internet karena seringkali sulit bagi pengguna untuk mengidentifikasi aktivitas tersebut [5].

Kasus phising di Indonesia banyak terjadi di e-commerce seperti Tokopedia, Shopee, Bukalapak, dll. Menurut Dara (2021), pengguna bisnis Shopee telah kehilangan hingga Rp.8.600.000 karena penipuan phising. Modus yang digunakan pelaku adalah menelepon, menginformasikan kepada korban bahwa mereka telah menerima hadiah, setelah itu pelaku mengirimkan link kepada korban dan meminta korban untuk memasukkan kode one time password (OTP) yang dikirimkan melalui SMS [11].

Kasus phising terhadap dunia e-commerce mendorong para peneliti untuk menyelidiki deskripsi serangan phising, jenis phising, dan cara pencegahan kejahatan phising. Banyak penelitian telah dilakukan

https://doi.org/10.32502/digital.v6i2.5653

pada serangan phising di sektor keuangan. Oleh karena itu, penelitian ini menganalisis kejahatan phising pada industri belanja online dengan menggunakan metode literature review. Ini bertujuan untuk menganalisis apa saja yang menyebabkan terjadinya phising di sektor e-commerce (studi kasus di marketplace Shoppe) dan memberikan rekomendasi tentang cara menghindari ancaman phising.

Metode Penelitian

a. Cybercrime

Sejarah cybercrime tidak dapat dipisahkan dari sejarah perkembangan teknologi. Munculnya kejahatan di dunia maya atau lebih dikenal dengan istilah “cybercrime” dimulai pada tahun 1988. Pada tahun tersebut, seorang mahasiswa berhasil membuat worm atau virus yang menyerang program komputer dan melumpuhkan sekitar 10% dari seluruh komputer di dunia yang terhubung ke internet.

Cybercrime merupakan kejahatan yang dilakukan dengan menggunakan teknologi informasi sebagai kejahatan utama. Cybercrime memanfaatkan perkembangan teknologi informasi, khususnya internet. Cybercrime didefinisikan sebagai penggunaan ilegal teknologi informasi berdasarkan kemajuan teknologi internet [1].

Adapun cybercrime dapat dikelompokkan menjadi sebagai berikut [1]:

1) Cyberpiracy: menggunakan teknologi computer untuk mencetak ulang perangkat lunak atau data dan kemudian mendistribusikan data atau perangkat lunak tersebut dengan menggunakan teknologi computer.
2) Cybertrespass: penggunaan teknologi komputer untuk meningkatkan akses ke system computer organisasi atau individu.
3) Cybervandalism: penggunaan teknologi komputer untuk membuat program yang mengganggu proses transmisi elektronik, dan merusak data di komputer.

b. Phising

Menurut Victoria (2013:214) Phishing (Password Harvesting Fishing) adalah aktivitas penipuan yang menggunakan email atau situs web palsu untuk mengelabui pengguna agar memungkinkan perlaku memperoleh informasi pengguna [6]. Selain itu Phishing dapat didefinisikan sebagai tindakan yang ditujukan untuk menemukan informasi rahasia dengan mengirimkan pesan palsu kepada pengguna melalui sarana komunikasi elektronik (Mustaqim, 2020). Kegiatan penipuan ini berupa email yang seolah-olah berasal dari sebuah perusahaan dan bertujuan untuk mendapatkan informasi pribadi pengguna berupa PIN, nomor rekening, nomor, dll [8].

Kemudian definisi lain dari phishing adalah istilah yang mengacu pada berbagai tindakan penjahat dunia maya dengan memberikan tautan kepada pengguna internet untuk tujuan mencuri data pribadi seperti perbankan, PIN, dan data di jejaring sosial. Metode umum yang digunakan untuk menipu pengguna online adalah dengan memberikan tautan atau email. Aktivitas phishing telah menimbulkan minat penelitian di komunitas keamanan internet karena seringkali sulit bagi pengguna untuk mengenali perilaku ini. [5].

Pandangan lain adalah bahwa phishing adalah kegiatan kriminal yang menggunakan teknik penipuan sosial. Phishing berupaya untuk secara curang mendapatkan informasi sensitif seperti nama pengguna, sandi, dan informasi kartu kredit dengan menyamar sebagai pihak tepercaya dalam komunikasi elektronik. Phishing menyerang semua aspek industri internet seperti: e-commerce, jejaring sosial dan perbankan. Serangan phishing menargetkan data pengguna yang sensitif untuk penggunaan yang tidak sah. Pengguna menderita perlindungan data, penyalahgunaan fungsi kode, dan bahkan kerugian finansial [15].

Phishing artinya memancing untuk mengumpulkan password. Penipuan phishing yang dirancang untuk mendapatkan informasi sensitif seperti kata sandi atau nomor kartu kredit, atau mengelabui orang agar mengunduh file yang berisi virus dengan menyamar sebagai orang yang dapat dipercaya secara komersial dalam komunikasi elektronik resmi seperti email atau pesan teks lain atau pengeluaran organisasi.

Dari beberapa pendapat di atas, dapat disimpulkan bahwa phising adalah upaya penipuan untuk mencuri informasi pribadi seperti password, nomor kartu kredit dan informasi sensitif lainnya dengan memberikan link atau email palsu. Phishing juga dikenal sebagai spoofing merek atau kartu, adalah bentuk layanan yang menipu korban dengan menjanjikan legitimasi dan keamanan transmisi data [7].

c. E-Commerce

Electronic commerce (e-commerce) adalah kegiatan distribusi, pembelian, penjualan dan pemasaran barang dan jasa melalui sistem elektronik seperti internet atau televisi, www atau jaringan komputer lainnya. Perdagangan elektronik dapat mencakup transfer uang elektronik, pertukaran data

P-ISSN : 2686-4185
E-ISSN : 2714-9706

elektronik, sistem manajemen inventaris otomatis, dan sistem entri data otomatis. E-commerce adalah penggunaan teknologi informasi yang dapat meningkatkan hubungan antara perusahaan dengan pelanggannya [2], [3].

E-commerce juga didefinisikan sebagai area perdagangan atau pertukaran informasi antara penjual dan pembeli di dunia maya (Indrajit, 2016). Munculnya perdagangan elektronik tidak terlepas dari pesatnya perkembangan teknologi informasi, khususnya internet. Dengan bantuan e-commerce, perusahaan dapat memasarkan produk atau layanannya ke seluruh dunia tanpa membatasi batasan geografis. Electronic commerce adalah salah satu pelopor munculnya prinsip ekonomi baru yang sekarang dikenal sebagai ekonomi digital. E-commerce lahir untuk memenuhi kebutuhan gaya hidup masyarakat modern yang menuntut kemudahan dan kecepatan dalam segala hal.

Penelitian ini menggunakan pendekatan kualitatif dengan metode literature review. Menurut Danial dan Warsiah (2009: 80), studi literatur (literature review) adalah penelitian yang dilakukan oleh akademisi dengan mengumpulkan sejumlah buku dan artikel yang berkaitan dengan masalah dan tujuan penelitian. Analisis data dalam penelitian ini dilakukan dengan cara mengumpulkan beberapa bahan dari buku, jurnal penelitian atau sumber lain untuk kemudian dianalisis dan disimpulkan dalam suatu pembahasan tentang hasil penelitian. Selain memanfaatkan website Mediakonsumen.com sebagai wadah pengaduan konsumen menghadapi berbagai masalah diantaranya penipuan online (phising) di industri e-commerce di marketplace Shopee.

Hasil dan Pembahasan

a) Kasus Kejahatan Phising di Sektor E-Commerce

Kasus penipuan di Indonesia banyak terjadi di industri e-commerce, seperti Tokopedia, Shopee, Bukapak, dll. Pada tahun 2020, terjadi kasus penipuan di platform e-commerce Shopee dengan modus penjual membatalkan pesanan yang dilakukan dengan alasan asuransi barang agar segera dikirim. Pelaku kemudian mengirimkan link phising melalui aplikasi WhatsApp kepada pengguna untuk melakukan transaksi pembayaran melalui link tersebut. Tiga menit sebelum transaksi pembayaran, pesanan dibatalkan oleh penipu [12].

Pada tahun 2021, pengguna e-commerce Shopee kembali mengalami kerugian hingga Rp 8.600.000 akibat aksi penipuan pencurian. Cara yang dilakukan penyerang adalah melakukan panggilan, memberitahukan kepada korban bahwa hadiah telah diterima, kemudian penyerang mengirimkan link kepada korban dan meminta kode OTP yang dikirimkan melalui SMS [11].

Lalu, di tahun yang sama 2021, terjadi kasus kejahatan phising dimana seorang pelaku yang mengaku sebagai penjual mengirimkan pesan singkat kepada seorang user tentang pesanannya. Pelaku merasa bahwa layanan pengiriman yang dipilih mengalami gangguan. Kemudian pengguna diminta untuk mengubah layanan pengiriman melalui tautan yang dikirimkan oleh pelaku. Pengguna mengisi semua data yang diperlukan termasuk PIN Shopeepay miliknya. Pengguna tidak mengetahui bahwa tautan tersebut adalah link phishing. Saat itu pelaku masuk ke akun shopee pengguna dan memiliki pinjaman shopee (Shopee Paylater) senilai Rp 3 juta. Pengguna segera menghubungi Customer Service (CS) Shopee dan tidak butuh waktu lama bagi pihak e-commerce terkait untuk menyelesaikan masalah tersebut [14].

b) Cara Kerja Phising

Informasi yang diperoleh atau dicari oleh penipu berupa password akun korban atau nomor kartu kredit. Penipu menggunakan email, spanduk, atau pop-up untuk mengelabui pengguna agar mengarahkan mereka ke situs web palsu. Situs web palsu adalah maket dari situs web asli yang ditargetkan dan selalu berisi kolom input (misalnya kotak teks). Saat pengguna mengirimkan informasi pribadi, informasi tersebut bocor ke penipu. Penipu memanfaatkan kecerobohan dan ketidakakuratan pengguna di situs web palsu populer untuk mendapatkan informasi [7].

Phishing adalah upaya untuk mendapatkan informasi sensitif pengguna melalui email dan situs web palsu dengan menyamar sebagai situs web resmi atau asli. Phishing memanipulasi tautan agar terlihat seperti alamat situs web asli. Trik yang umum digunakan oleh scammer adalah menggunakan subdomain palsu dan URL rusak [4].

Phishing memanipulasi tautan agar terlihat seperti alamat situs web asli. Trik umum yang digunakan penipu adalah menggunakan subdomain palsu dan URL yang salah format, seperti URL www.shopee.co.id diganti dengan www.shopee.net. Penulis akan meyakinkan pengguna untuk mengungkapkan informasi pribadi mereka melalui halaman palsu yang terlihat seperti halaman aslinya melalui email yang dikirimkan oleh penulis. Situs web ini diadaptasi semirip mungkin dengan situs web asli sehingga pengguna dapat mempercayainya dan mengirimkan informasi pribadi mereka.

c) Teknik Phising

Dalam memikat korbannya, phiser menggunakan teknik berikut [7]:

1) Email spoofing, teknik yang sering digunakan oleh phiser untuk mengirim email ke jutaan pengguna dengan menyamar berasal dari institusi yang sah. Email tersebut biasanya berisi permintaan nomor kredit, password, atau mengunduh formulir tertentu (Joshi, 2012:5)
2) Pengiriman berbasis web adalah salah satu teknik phising paling canggih. Dikenal juga dengan istilah "man-in-the-middle". Hacker berada diantara situs web asli dan system phising.
3) Pesan instan (chatting) dimana pengguna menerima pesan dengan tauran yang mengarahkan mereka ke situs web phising palsu yang terlihat dan terasa seperti situs web resmi.
4) Trojan hosts, hacker terlihat mencoba untuk masuk ke akun pengguna untuk mengumpulkan kredensial menggunakan komputer lokal. Informasi yang diperoleh kemudian dikirim ke phiser.
5) Manipulasi tautan (link), phiser mengirimkan link ke situs web. Ketika pengguna mengklik link tersebut situs web phiser akan terbuka bukan tautan situs web yang sebenarnya.
6) Malware phising, phiser melibatkan malware memerlukan cara untuk dijalankan pada computer pengguna. Malware ini biasanya melekat pada email phising yang dikirim ke pengguna. Saat korban mengklik tautan tersebut, malware mulai berjalan. Malware terkadang disertakan dalam file unduhan.

d) Penyebab Terjadinya Phising pada Sektor E-Commerce

Adapun factor terjadinya phising dalam sektor e-commerce yaitu sebagai berikut [9]:

1) Pengetahuan pengguna yang minim

Perlunya edukasi kepada seluruh lapisan masyarakat untuk mengetahui adanya ancaman phising pada layanan e-commerce. perlu adanya sosialisasi dan pemberitahuan kepada seluruh masyarakat untuk mengetahui adanya ancaman penipuan dalam transaksi digital.Pengetahuan pengguna terhadap domain, link atau website palsu yang menyerupai aslinya sangat minim, sehingga pengguna tidak menyadari bahwa telah menggunakan situs web palsu [13].

2) Kebocoran data pengguna

Perlu diperhatikan akan data pribadi tidak bocor adalah, jangan pernah memberi data pribadi seperti: KTP, SIM, nomor rekening, kode vertifikasi, dan data pribadi lainnya. Apabila data pribadi kita telah tersebarkan, orang tak bertanggung jawab dapat menggunakannya untuk tindakan yang tak bertanggung jawaban. Hacker memanfaatkan data kita melalui link atau situs situs online. Jadi, jika kalian mendapatkan link atau email yang tidak pasti isinya apa, jangan pernah membuka link tersebut, karena itu bisa saja jebakan dari hacker untuk melakukan tindakannya.

3) Pengguna tergiur dengan hadiah palsu atau promosi

Segelintir orang ada sudah paham adanya penipuan dalam transaksi online, namun masih saja terjebak dengan kasus tersebut. Hal ini biasanya disebabkan oleh, tergiurnya pengguna oleh iming – iming hadiah puluhan juta rupiah ataupun barang mewah lainnya.

Abroshan et al., (2018) mengungkapkan bahwa pelaku menggunakan kelemahan pengguna dengan menawarkan promosi yang menarik serta mengelabui pengguna agar dapat memenuhi keinginan pelaku. Pelaku menargetkan psikologis pengguna, dan menggunakan kelemahan tersebut untuk membangun kepercayaan pengguna. Hal ini menyebabkan pengguna dengan mudah terjebak dengan hadiah atau promosi yang di berikan pelaku melalui email palsu [10].

4) Sistem keamanan dan kurang tegasnya kebijakan pemerintah

Kasus kebocoran data pada aplikasi e-commerce, menunjukkan sistem keamanan e-commerce Indonesia yang tidak aman. Kurang tegasnya kebijakan pemerintah dalam hal ini, menjadikan kesempatan bagi para cybercrime. Padahal di Indonesia sendiri sudah ada beberapa undang – undang dan menteri kominfo yang mengawasi keamanan transaksi e-commerce. Namun kebijakan tersebut belum sepenuhnya berhasil, hal itu dapat dibuktikan dengan kasus – kasus penipuan yang marak terjadi. Kita sebagai masyarakat biasa, apabila mendapatkan kasus tersebut, kita berhak melaporkan tindakan tersebut kepada pihak berwajib guna mengurangi angka penipuan dalam transaksi e-commerce.

5) Mencegah Serangan Kejahatan Phising

Berikut adalah beberapa tips yang harus dihindari atau mencegah terjadinya phising pada penggunaan layanan e-commerce:

a) Periksa dengan cermat URL atau alamat yang sedang Anda tuju, pastikan alamat di Address bar sudah benar bahwa alamat tersebut adalah alamat yang Anda tuju.
b) Biasakan mengetik URL atau alamat website yang Anda tuju dan hindari link Web yang menurut Anda mencurigakan.

P-ISSN : 2686-4185
E-ISSN : 2714-9706

c) Ganti password secara berkala, baik dalam 1 minggu, 2 minggu, 1 bulan atau dalam periode tertentu. Ini berguna untuk mempersulit pelacakan password Anda.
d) Jangan pernah menanggapi email yang mencurigakan apalagi memasukkan kata sandi pada situs web yang mencurigakan atau tidak dapat dipercaya dan mengirimkan kata sandi dan informasi pribadi penting melalui email. Situs web atau bisnis yang sah biasanya tidak meminta informasi melalui email.
e) Jika Anda menerima permintaan informasi rahasia, buka browser baru dan buka situs web organisasi dengan mengetikan alamat situs web organisasi untuk memastikan itu adalah situs web organisasi yang sebenarnya dan bukan situs web phiser. Jika Anda membutuhkan sesuatu, biasanya ada pengumuman di situs web organisasi atau jika Anda tidak yakin dengan permintaan ini, hal terbaik adalah pergi ke situs web organisasi untuk memeriksanya.
f) Jangan pernah membuka situs web yang mencurigakan atau tidak Anda percayai. Periksa URL untuk memastikan halaman tersebut benar-benar bagian dari situs web organisasi dan bukan halaman palsu di domain lain seperti www.shopee.net.
g) Waspada terhadap penawaran fantastis yang tampaknya terlalu mudah untuk menjadi kenyataan, bisa jadi itu phiser.
h) Gunakan browser yang filter phising untuk mengidentifikasi potensi serangan phising. Alamat situs web aman dimulai dengan “https://” dan menunjukan gembok tertutup di browser Anda.

Simpulan

Phishing merupakan ancaman yang menggunakan teknik rekayasa sosial dengan menyamar sebagai orangyang berwenang, menjadi penjual ataupun menjadi pihak dari e-commerce itu sendiri. Dari sekian banyak Literature Review, menyatakan bahwa faktor peyebab terjadinya phishing pada layanan e-commerce adalah minimnya pengetahuan pengguna, serta privasi social network service. Dampak dari kejahatan phishing mengakibatkan kerugian finasial, pencurian identitas seseorang dan pembobolan akun. Dengan demikian dilakukanlah pencegahan serangan phishing pada layanan e-commerce. Pencegahan yang dilakukan adalah edukasi kepada pengguna, pengguna yang telah mendapatkan edikasi akan dengan mudah mendeteksi dan menghindari ancaman phishing yang terdapat pada e-mail dan URL atau situs web. Melakukan pencegahan serangan phishing di level e-mail, menggunakan aplikasi (software) anti-phishing, serta menggunakan sistem kode verifikasi (OTP) untuk melindungi keamanan informasi dan akun pengguna. Namun, hal ini dikembalikan lagi kepada pengguna apakah akan merespon atau mengabaikan pesan tersebut saat menggunakan transaksi online (ecommerce).

Daftar Pustaka

[1] T. Sutabri, *KOMPUTER dan MASYARAKAT*, 1 ed. Yogyakarta: Andi, 2013.
[2] T. Sutabri, *SISTEM INFORMASI BISNIS*, 1 d. Yogyakarta: Andi, 2019
[3] A.N Salim dan T. Sutabri “Analisis IT Service Management (ITSM) pada Layanan Marketplace Shopee Menggunakan Framework ITIL V3,” *Jurnal Nuansa Informatika.*, vol. 17, no. 2, hlm. 15, Jan 2023, doi: https://doi.org/10.25134/nuansa
[4] I.H. Ramadhan, dan E.K. Nurnawati “Analisis Ancaman *Phising* dalam Layanan *E-commerce”, Prosiding Seminar Nasional Aplikasi Sains & Teknologi (SNAST),* hlm. E-32, Nov 2022
[5] A.S Sunge “Komparasi *Machine Learning* Memprediksi *Phising* dalam Keamanan *Website”, Prosiding SAINTEK : Sains dan Teknologi,* vol. 1, no.1, hlm, 135, Juli 2022
[6] Dedi Irawan “Mencuri Informasi Penting Dengan Mengambil Alih Akun Facebook denagn Metode *Phising”, Jurnal Ilmu Komputer & Informatika,* vol. 1, no. 1, hlm. 44, Juli 2020
[7] D. Rachmawati “*Phising* sebagai Salah Satu Bentuk Ancaman dalam Dunia *Cyber”, Jurnal Ilmiah SAINTIKOM,* vol. 13, no. 3, September 2014
[8] F. N. Latifah, dkk “Ancaman Pencurian Data *(Phising)* di Tengah Pengguna Fintech pada Pandemic Covid-19 *(Study Phising di Indonesia),* vol. 6(1), hlm. 77, Maret 2022, doi : 10.21070/perisai.v6i1.1598
[9] P.R. Silalahi, dkk “Analisis Keamanan Transaksi E-Commerce dalam Mencegah Penipuan *Online”, Profit : Jurnal Manajemen, Bisnis dan Akuntansi,* vol. 1, no. 4, hlm.229, Nov 2022.
[10] Abroshan, H., Devos, J., Poels, G., & Laermans, E. “*Phishing attacks root causes. In Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes ini Bioinformatics), Springer International Publishing*, 2018, vol. 10694 https://doi.org/10.1007/978-3-319-76687-4_13
[11] Dara. Akun *Shopee Dibajak Penipu Hampir Puluhan Juta Rupiah!* 2021. *Mediakonsumen.com.* https://mediakonsumen.com/2021/05/01/surat-pembaca/akun-shopee-dibajak-penipu-hampir-puluhan-jutarupiah
[12] Suaib, I. Modus Penipuan oleh Penjual di Shopee. 2020. *Mediakonsumen.com.* https://mediakonsumen.com/2022/01/07/surat-pembaca/modus-penipuan-oleh-penjual-di-shopee-2

[13] Muftiadi, A., Putri, dkk "Studi Kasus Keamanan Jaringan Komputer : Analisis Ancaman *Phising* Terhadap Layanan *Online Banking*, 1(2), hlm. 60-65, 2022
[14] Faliha, A. Cerita Elma Theana Tertipu saat Belanja *Online*, Alami Kerugian Jutaan Rupiah. 2021. Merdeka.com.
[15] N.P Singh, P "*Online Frauds in Banks with Phishing", Journal of Internet Banking and Commerce,* p.4, 2007